



- 1 -

#1b

**Practitioner's Docket No. XACTP001 *PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of )  
Givoly ) Group Art Unit: 2155  
Application No. 09/924,391 ) Examiner: Tran, Philip B.  
Filed: 08/07/01 ) Attorney Docket No. XACTP001  
For: SYSTEM, METHOD AND COMPUTER)  
PROGRAM PRODUCT FOR )  
PROCESSING NETWORK )  
ACCOUNTING INFORMATION )

**Commissioner for Patents  
Alexandria, VA 22313-1450**

RECEIVED

JUN 30 2004

## Technology Center 2100

**ATTENTION: Board of Patent Appeals and Interferences**

**APPELLANT'S BRIEF (37 C.F.R. § 1.192)**

This brief is in furtherance of the Notice of Appeal, filed in this case on April 20, 2004.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate. (37 C.F.R. § 1.192(a))

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 1.192(c)):

- I REAL PARTY IN INTEREST
- II RELATED APPEALS AND INTERFERENCES
- III STATUS OF CLAIMS
- IV STATUS OF AMENDMENTS
- V SUMMARY OF INVENTION
- VI ISSUES
- VII GROUPING OF CLAIMS
- VIII ARGUMENTS

#### APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

06/28/2004 X0011TE1 00000108 09924391

01 FC-2402

165.00 DP

The final page of this brief bears the practitioner's signature.

**I REAL PARTY IN INTEREST (37 C.F.R. § 1.192(c)(1))**

The real party in interest in this appeal is Xacct Technologies, Ltd.

**II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 1.192(c)(2))**

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals or interferences.

**III STATUS OF CLAIMS (37 C.F.R. § 1.192(c)(3))**

**A. TOTAL NUMBER OF CLAIMS IN APPLICATION**

Claims in the application are: 1-23.

**B. STATUS OF ALL THE CLAIMS IN APPLICATION**

1. Claims withdrawn from consideration but not canceled: None
2. Claims pending: 1-23
3. Claims allowed: None
4. Claims rejected: 1-23

**C. CLAIMS ON APPEAL**

The claims on appeal are: 1-23

**IV STATUS OF AMENDMENTS (37 C.F.R. § 1.192(c)(4))**

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

#### **V SUMMARY OF INVENTION (37 C.F.R. § 1.192(c)(5))**

As set forth in Figure 4 and the accompanying description of the originally filed specification, a method and computer program product are provided for processing network accounting information. Accounting information is initially received over a packet-switched network. Note operation 402 in Figure 4 and the accompanying description. At least one aspect of the received accounting information is then monitored. In use, at least a portion of the accounting information that occurs during a surge in network traffic is discarded, based on the monitored aspect. Note operation 402 in Figure 4 and the accompanying description.

#### **VI ISSUES (37 C.F.R. § 1.192(c)(6))**

Issue # 1: The Examiner has rejected Claims 1-4, 6-8, 10-17, and 20-22 under 35 U.S.C. 102(e) as being anticipated by Conklin et al. (USPN 5,991,881).

Issue # 2: The Examiner has rejected Claims 5 and 18 under 35 U.S.C. 103(a) as being unpatentable over Conklin et al. (USPN 5,991,881) in view of Savoldi et al. (USPN 5,727,146).

Issue # 3: The Examiner has rejected Claims 9 and 19 under 35 U.S.C. 103(a) as being unpatentable over Conklin et al. (USPN 5,991,881) in view of Trcka et al. (USPN 6,453,345).

Issue # 4: The Examiner has rejected Claim 23 under 35 U.S.C. 103(a) as being unpatentable over Conklin et al. (USPN 5,991,881) in view of Savoldi et al. (USPN 5,727,146) and further in view of Trcka et al. (USPN 6,453,345).

## **VII GROUPING OF CLAIMS (37 C.F.R. § 1.192(c)(7))**

The claims of the groups below do not stand or fall together. Following is the grouping of claims. In the following section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1: Grouping of Claims –

Group #1: Claims 1, 2, 6, 10-12, 15, and 20.

Group #2: Claim 3 and 13.

Group #3: Claim 4 and 14.

Group #4: Claim 7 and 16.

Group #5: Claim 8 and 17.

Group #6: Claim 21-22.

Issue # 2: Grouping of Claims –

Group #1: Claims 5 and 18.

Issue # 3: Grouping of Claims –

Group #1: Claims 9 and 19.

Issue # 4: Grouping of Claims –

Group #1: Claim 23.

## **VIII ARGUMENTS (37 C.F.R. § 1.192(c)(8))**

Issue #1:

The Examiner has rejected Claims 1-4, 6-8, 10-17, and 20-22 under 35 U.S.C. 102(e) as being anticipated by Conklin et al. (USPN 5,991,881).

*Group #1: Claims 1, 2, 6, 10-12, 15, and 20*

With respect to the first claim grouping, the Examiner argues that appellant misinterprets the terminologies when comparing the limitations of the independent claims with appellant's quoted paragraph from Conklin. Moreover, the Examiner now relies on the abstract and col. 6, lines 40-43 from Conklin to meet appellant's claimed "discarding at least a portion of the accounting information that occurs during a surge in network traffic, based on the monitored aspect." Following are such excerpts.

"This is a system and method for network surveillance and detection of attempted intrusions, or intrusions, into the network and into computers connected to the network. The System functions are: (A) intrusion detection monitoring, (B) real-time alert, (C) logging of potential unauthorized activity, and (D) incident progress analysis and reporting. Upon detection of any attempts to intrude, the System will initiate a log of all activity between the computer elements involved and send an alert to a monitoring console. When a log is initiated, the network continues to be monitored by a primary surveillance system. A secondary monitoring process is started which interrogates the activity log in real-time and sends additional alerts reporting the progress of the suspected intruder." (Abstract)

"Third party evidence logging provides reliable data for determining appropriate response activities, such as restoring lost data, removing unauthorized programs, or disconnecting the system from the network temporarily." (col. 6, lines 40-43)

The Examiner summarizes appellant's arguments as being merely based on the "discarded" limitation. Appellant respectfully disagrees, as appellant teaches and claims "discarding at least a portion of the accounting information that occurs during a surge in network traffic, based on the monitored aspect," not just "discarding," as purported by the Examiner.

It appears that the Examiner is relying on Conklin's "disconnecting the system from the network temporarily" language to meet appellant's claimed "discarding."

Appellant asserts, however, that such excerpts from Conklin are merely suggesting disconnecting network traffic, and not discarding "network accounting information" (emphasis added).

In use, network accounting information processors collect network accounting information relating to network traffic. In case of a surge in network traffic, such accounting information associated with the network traffic may become overly cumbersome for processor resources (i.e. memory, etc.).

Thus, appellant teaches and claims a technique of dealing with "network accounting information" overflow, as opposed to the overflow of the *traffic itself*, in order to prevent overflow of this particular type of information during a surge in network traffic, by discarding the same. It is noted that Conklin would prevent overall communication of the *network traffic itself* via the network by virtue of its "disconnecting," while appellant's claimed invention may optionally allow such communication, while still avoiding "network accounting information" overflow.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Conklin reference, at least in part, because it does not disclose "discarding network accounting information" based on a monitored aspect during a surge in network traffic, as claimed.

*Group #2: Claim 3 and 13*

With respect to the present grouping, the Examiner continues by relying on Figure 6 to make a prior art showing of appellant's claimed "wherein the accounting information is discarded for dealing with heavy network traffic." After careful of Figure 6, it clearly fails to disclose, teach or even suggest such limitations.

Again, Conklin deals with network attacks, not "dealing with heavy network traffic," by discarding accounting information, as claimed.

*Group #3: Claim 4 and 14*

With respect to the present grouping, the Examiner relies on col. 4, line 52 – col. 5, line 45 to make a prior art showing of appellant's claimed "generating a summary of the accounting information." Such excerpts, however, do not disclose, teach or even suggest "accounting information", let alone "generating a summary of the accounting information," as claimed.

*Group #4: Claim 7 and 16*

With respect to the present grouping, the Examiner relies on col. 4, line 52 – col. 5, lines 30-67; and Figures 6-8 to make a prior art showing of appellant's claimed "wherein monitoring the at least one aspect of the received accounting information includes monitoring a rate of receipt of the accounting information." Such excerpts, however, do not disclose, teach or even suggest "a rate of receipt of the accounting information." Instead, there is a mere mention of a time of day, number and types of packets, common destination/source address combinations, etc. A number of packets constitutes an amount, not a "rate," as claimed.

*Group #5: Claim 8 and 17*

With respect to the present grouping, the Examiner relies on col. 4, line 52 – col. 5, lines 30-67; and Figures 6-8 to make a prior art showing of appellant's claimed "wherein monitoring the at least one aspect of the received accounting information includes detecting whether the rate of receipt of the accounting information exceeds a predetermined amount." Such excerpts, however, do not even disclose, teach or suggest "a rate of receipt of the accounting information." Instead, there is a mere mention of a time of day, number and types of packets, common destination/source address combinations, etc. It is noted that Conklin does not even suggest a "rate," let alone "detecting whether the rate of receipt of the accounting information exceeds a predetermined amount," as claimed.

*Group #6: Claim 21-22*

With respect to the present grouping, the Examiner simply dismisses such claim language by stating that it is rejected for reasons similar to Claim 1. Appellant respectfully disagrees with this assertion, since Claims 21 and 22 require "conditionally preventing an overload of the accounting information that occurs during a surge in network traffic, based on the monitored aspect," which is absent from both Claim 1 and Conklin.

Issue # 2:

*Group #1: Claims 5 and 18*

The Examiner has rejected Claims 5 and 18 under 35 U.S.C. 103(a) as being unpatentable over Conklin et al. (USPN 5,991,881) in view of Savoldi et al. (USPN 5,727,146).

With respect to the present grouping, the Examiner relies on the Abstract; col. 1, line 61 – col. 2, line 30; and col. 2, line 53 – col. 3, line 3 of Savoldi to make a prior art

showing of appellant's claimed "wherein monitoring the at least one aspect of the received accounting information includes detecting a scan of a plurality of ports." It appears that the Examiner has not taken into consideration the full weight of appellant's claims.

Specifically, such excerpts do not disclose, teach or even suggest port scanning in the specific context of "monitoring the at least one aspect of the received accounting information," as opposed to the *traffic itself*.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant thus respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the Examiner's proposed combination does not disclose, teach or suggest appellant's claim language, as set forth hereinabove.

Issue # 3:

*Group #1: Claims 9 and 19*

The Examiner has rejected Claims 9 and 19 under 35 U.S.C. 103(a) as being unpatentable over Conklin et al. (USPN 5,991,881) in view of Trcka et al. (USPN 6,453,345).

With respect to the present grouping, the Examiner relies on col. 21, lines 24-28 to make a prior art showing of appellant's claimed "wherein monitoring the at least one aspect of the received accounting information includes monitoring a load on a system receiving the accounting information." It appears that the Examiner has again not taken into consideration the full weight of appellant's claims.

Specifically, such excerpt simply suggest "peak loads," but does not disclose, teach or even suggest monitoring a load on a system receiving accounting information in the specific context of "monitoring the at least one aspect of the received accounting information includes monitoring a load on a system receiving the accounting information," as opposed to *the traffic itself*.

Again, the Examiner's cited reference monitors a load on a system receiving *traffic itself*, not a system receiving the accounting information, as claimed.

Appellant thus respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the Examiner's proposed combination does not disclose, teach or suggest appellant's claim language, as set forth hereinabove.

Issue # 4

*Group #1: Claim 23*

The Examiner has rejected Claim 23 under 35 U.S.C. 103(a) as being unpatentable over Conklin et al. (USPN 5,991,881) in view of Savoldi et al. (USPN 5,727,146) and further in view of Trcka et al. (USPN 6,453,345).

With respect to the present groupings, is noted that the Examiner's application of the prior art to this claim is replete with deficiencies. Just by way of example, with respect to Claim 23, the Examiner relies on Conklin's teaching that "network specific characteristics or facts may be developed from the network data collection over time and stored in a database" to meet appellant's claimed "detecting a rate of receipt of the accounting information [and] detecting whether the rate of receipt of the accounting information exceeds a predetermined amount."

However, the mere discussion of network specific characteristics "over time" does not rise to the level of specificity to meet appellant's claimed predetermined rate threshold-based discarding of accounting information. Moreover, it is noted that the Examiner simply looks to Trcka and Savoldi to meet appellant's claimed port scans and load detection. However, the proposed combination still fails to meet appellant's specific accounting information overload prevention technique involving the discarding of the same based on port scans and network load detection.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

## **IX APPENDIX OF CLAIMS (37 C.F.R. § 1.192(c)(9))**

The text of the claims involved in the appeal is:

1. (Previously Amended) A method for processing network accounting information, comprising:
  - (a) receiving accounting information over a packet-switched network;
  - (b) monitoring at least one aspect of the received accounting information; and
  - (c) discarding at least a portion of the accounting information that occurs during a surge in network traffic, based on the monitored aspect.
2. (Original) The method as recited in claim 1, wherein the accounting information is discarded for providing a defense against network attacks.
3. (Original) The method as recited in claim 1, wherein the accounting information is discarded for dealing with heavy network traffic.
4. (Original) The method as recited in claim 3, and further comprising generating a summary of the accounting information.
5. (Original) The method as recited in claim 1, wherein monitoring the at least one aspect of the received accounting information includes detecting a scan of a plurality of ports.
6. (Original) The method as recited in claim 1, wherein monitoring the at least one aspect of the received accounting information includes detecting a scan of a plurality of Internet Protocol (IP) addresses.

7. (Original) The method as recited in claim 1, wherein monitoring the at least one aspect of the received accounting information includes monitoring a rate of receipt of the accounting information.
8. (Original) The method as recited in claim 7, wherein monitoring the at least one aspect of the received accounting information includes detecting whether the rate of receipt of the accounting information exceeds a predetermined amount.
9. (Original) The method as recited in claim 1, wherein monitoring the at least one aspect of the received accounting information includes monitoring a load on a system receiving the accounting information.
10. (Original) The method as recited in claim 1, wherein the network includes the Internet.
11. (Previously Amended) A computer program product for processing network accounting information, comprising:
  - (a) computer code for receiving accounting information over a packet-switched network;
  - (b) computer code for monitoring at least one aspect of the received accounting information; and
  - (c) computer code for discarding at least a portion of the accounting information that occurs during a surge in network traffic, based on the monitored aspect.
12. (Original) The computer program product as recited in claim 11, wherein the accounting information is discarded for providing a defense against network attacks.
13. (Original) The computer program product as recited in claim 11, wherein the accounting information is discarded for dealing with heavy network traffic.

14. (Original) The computer program product as recited in claim 13, and further comprising computer code for generating a summary of the accounting information.
15. (Original) The computer program product as recited in claim 11, wherein the computer code for monitoring the at least one aspect of the received accounting information includes computer code for detecting a scan of a plurality of Internet Protocol (IP) addresses.
16. (Original) The computer program product as recited in claim 11, wherein the computer code for monitoring the at least one aspect of the received accounting information includes computer code for monitoring a rate of receipt of the accounting information.
17. (Original) The computer program product as recited in claim 16, wherein the computer code for monitoring the at least one aspect of the received accounting information includes computer code for detecting whether the rate of receipt of the accounting information exceeds a predetermined amount.
18. (Original) The computer program product as recited in claim 11, wherein the computer code for monitoring the at least one aspect of the received accounting information includes computer code for detecting a scan of a plurality of ports.
19. (Original) The computer program product as recited in claim 11, wherein the computer code for monitoring the at least one aspect of the received accounting information includes computer code for monitoring a load on a system receiving the accounting information.

20. (Previously Amended) A system for processing network accounting information, comprising:
  - (a) logic for receiving accounting information over a packet-switched network;
  - (b) logic for monitoring at least one aspect of the received accounting information; and
  - (c) logic for discarding at least a portion of the accounting information that occurs during a surge in network traffic, based on the monitored aspect.
21. (Previously Amended) A method for processing network accounting information, comprising:
  - (a) receiving accounting information over a packet-switched network;
  - (b) monitoring at least one aspect of the received accounting information; and
  - (c) conditionally preventing an overload of the accounting information that occurs during a surge in network traffic, based on the monitored aspect.
22. (Previously Amended) A method for processing network accounting information, comprising:
  - (a) receiving accounting information over a packet-switched network;
  - (b) receiving an indication relating to at least one aspect of the received accounting information; and
  - (c) conditionally preventing an overload of the accounting information that occurs during a surge in network traffic, based on the indication.

23. (Previously Amended) A method for processing network accounting information, comprising:

- (a) receiving accounting information over a packet-switched network;
- (b) detecting a scan of a plurality of ports;
- (c) detecting a scan of a plurality of Internet Protocol (IP) addresses;
- (d) detecting a rate of receipt of the accounting information;
- (e) detecting whether the rate of receipt of the accounting information exceeds a predetermined amount;
- (f) detecting a load on a system receiving the accounting information;
- (g) conditionally preventing an overload of the accounting information based on aspects detected during steps (b)-(f); and
- (h) generating a summary of the accounting information;
- (i) wherein the accounting information that occurs during a surge in network traffic is discarded.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. XACTP001).

Respectfully submitted,

By: \_\_\_\_\_

Kevin J. Zilka

Reg. No. 41,429

Date: 10/21/01

Silicon Valley IP Group, P.C.  
P.O. Box 721120  
San Jose, California 95172-1120  
Telephone: (408) 971-2573  
Facsimile: (408) 971-4660



AF 2155  
83  
PATENT  
#16  
LDJ  
7-7-04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Tal Givoly

Application No.: 09/924,391

Filed: 08/07/2001

For: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR PROCESSING  
NETWORK ACCOUNTING INFORMATION

Group No.: 2155

Examiner: Philip B. Tran

Mail Stop Appeal Briefs – Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF  
(PATENT APPLICATION--37 C.F.R. § 1.192)

1. Transmitted herewith, in triplicate, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on April 20, 2004.
2. STATUS OF APPLICANT

This application is on behalf of a small entity.

RECEIVED

JUN 30 2004

Technology Center 2100

---

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10\*

(When using Express Mail, the Express Mail label number is **mandatory**;  
Express Mail certification is **optional**.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)  
with sufficient postage as first class mail.

37 C.F.R. § 1.10\*  
as "Express Mail Post Office to Addressee"  
Mailing Label No. \_\_\_\_\_ (mandatory)

TRANSMISSION

facsimile transmitted to the Patent and Trademark Office, (703) \_\_\_\_\_

Erica L. Farlow  
Signature

Date: 6/21/2004

Erica L. Farlow

(type or print name of person certifying)

\* Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 1.17(c), the fee for filing the Appeal Brief is:

small entity \$165.00

**Appeal Brief fee due \$165.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	\$165.00
Extension fee (if any)	\$0.00

**TOTAL FEE DUE \$165.00**

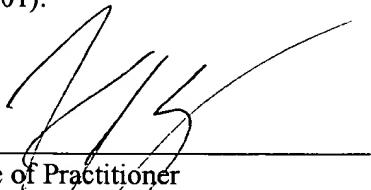
6. FEE PAYMENT

Attached is a check in the amount of \$165.00.

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. XACTP001).



Signature of Practitioner

Kevin J. Zilka  
Silicon Valley IP Group, PC  
P.O. Box 721120  
San Jose, CA 95172-1120  
USA

Reg. No.: 41,429  
Tel. No.: 408-971-2573  
Customer No.: 28875